UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

_____

Ex parte BRETT B. BONNER and RANDALL J. JACKSON

_____

Appeal 2007-1806
Application 09/836,350[1]
Technology Center 2600

_____

Decided: October 31, 2007

_____

Before JOSEPH F. RUGGIERO, HOWARD B. BLANKENSHIP, and
MARC S. HOFF, *Administrative Patent Judges*.

HOFF, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF CASE

   Appellants appeal under 35 U.S.C. § 134 from a Final Rejection of
claims 1-28. We have jurisdiction under 35 U.S.C. § 6(b).

   We reverse.

   Appellants' invention relates to a system and method for controlling
access to a designated area, especially by an agent delivering one or more

_____

items to a customer who may not be present for the delivery. Different codes are generated and delivered to the agent and customer respectively. Agent and customer enter other pieces of transaction-related data, which are combined with their initial key to produce an "access key" and "validation key," which must match in order for access to the designated area to be granted to the agent (Specification 1-3).

Claim 20 is exemplary:

20. A method for controlling access to a designated area, the designated area having a security device to control access thereto, comprising the steps of:

generating a first and second key for each access to the designated area;

using the first key, generating an access key;

using the second key, generating a validation key; and

comparing the access key and the validation key and causing the security device to allow access to the designated area if the access key matches the validation key.

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Holcomb	5,670,940	Sep. 23, 1997
Porter	5,774,053	Jun. 30, 1998
Lee	6,367,011 B1	Apr. 02, 2002
		(Filed Oct. 13, 1998)
Scott	6,484,260 B1	Nov. 19, 2002
		(Filed Apr. 24, 1998)

Claims 1-3, 12 and 20 stand rejected under 35 U.S.C. § 102(b) as being obvious over Holcomb.

Claims 4, 9 and 14 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Holcomb in view of Lee.

Claim 13 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Holcomb in view of Scott.

Claims 5-8, 10, 11, 15-19 and 26-28 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Holcomb in view of Lee and Porter.

The rejection of claims 21-25 was withdrawn by the Examiner.

Appellants contend that the Examiner erred in her rejection of the claims, because Holcomb does not teach generating a validation key based upon a second key, as claimed by Appellants in independent claims 1 and 20. The Examiner contends that the claims are properly rejected because the key generating station of Holcomb generates a first and second key, according to the broadest reasonable interpretation of Appellants' claims.

Rather than repeat the arguments of Appellants or the Examiner, we make reference to the Briefs and the Answer for their respective details. Only those arguments actually made by Appellants have been considered in this decision. Arguments that Appellants could have made but chose not to make in the Briefs have not been considered and are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(vii).

<div align="center">ISSUE</div>

The principal issue in the appeal before us is whether the Examiner erred in holding that Holcomb teaches a programmable unit that generates a first and second key for each access to the designated area, the first key being used to generate an access key and the second key being used to generate a validation key.

<div align="center">3</div>

FINDINGS OF FACT

The following Findings of Fact (FF) are shown by a preponderance of the evidence.

The Invention

1.   Appellants invented a system and method for controlling access to a designated area, especially by an agent delivering one or more items to a customer who may not be present for the delivery (Specification 1).

2.   A programmable unit generates an agent key and a customer key for each access to a designated area (Specification 5).

3.   The agent enters the agent key, its agent code, the access date, and the customer's address into a programming unit, which in response generates an encrypted access key stored on the agent's programmable tag (Specification 8-9).

4.   The customer enters the customer key, the agent code, the address of the designated area, and the access date into the validation system, which then generates and stores an encrypted validation key, to be matched against the access key when it is presented. Access is granted if the access key and validation key match (Specification 9-10).

Holcomb

5.   Holcomb teaches an electronic lock system which automatically blocks access to a room by hotel staff when a guest is in the room (col. 2).

6.   Holcomb teaches a key generating station at the front desk of a hotel, which encodes an access key code onto a magnetic media bearing card (col. 1, ll. 23-26).

7.   Each room door has an electronic lock, which is equipped with a microcontroller. The microcontroller is alternately (a) hard-wired to the key generating station to receive the access key code from the station; (b) equipped with the same algorithm as the key generating station, such that it can calculate the correct code; or (c) set up to contain the same codes in its storage as the key generating station (col. 1, ll. 34-40).

Lee

8.   Lee teaches a process for speeding up the personalization of smart cards. Any needed derived card keys are derived prior to the time of personalization at the personalization bureau. Master (secret) keys are retained at the issuer's location, rather than transmitted to the personalization bureau, which provides greater overall security (col. 2-3).

Porter

9.   Porter teaches a lockable storage device with an enclosure for enclosing delivered goods, and a communication apparatus operably coupled with the enclosure for controlling entry to the enclosure and providing an indication that goods have been delivered to (or picked up from) the enclosure (col. 2).

Scott

10.   Scott teaches sensing a biometric trait (e.g. a fingerprint) of a user and providing a biometric signal indicative thereof. A processing circuit compares the biometric signal with stored biometric data. The processor provides a verification signal only if the biometric signal corresponds sufficiently to the biometric data to verify that the user is the enrolled person (col. 1).

PRINCIPLES OF LAW

Anticipation is established when a single prior art reference discloses expressly or under the principles of inherency each and every limitation of the claimed invention. *Atlas Powder Co. v. IRECO Inc.*, 190 F.3d 1342, 1347, 51 USPQ2d 1943, 1946 (Fed. Cir. 1999); *In re Paulsen*, 30 F.3d 1475, 1478-79, 31 USPQ2d 1671, 1673 (Fed. Cir. 1994).

In rejecting claims under 35 U.S.C. § 103, the Examiner bears the initial burden of establishing a prima facie case of obviousness. *In re Piasecki*, 745 F.2d 1468, 1472, 223 USPQ 785, 788 (Fed. Cir. 1984). The Examiner can satisfy this burden by showing some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *KSR Int'l. Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007) (*citing In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006)). Only if this initial burden is met does the burden of coming forward with evidence or argument shift to the Appellant. *Piasecki*, 745 F.2d at 1472, 223 USPQ at 788. Thus, the Examiner must not only assure that the requisite findings are made, based on evidence of record, but must also explain the reasoning by which the findings are deemed to support the Examiner's conclusion.

ANALYSIS

     Appellants argue that Holcomb does not anticipate the invention claimed in independent claims 1 and 20, because (a) there is no teaching of a "signal that causes the algorithm used … to generate the access key" in Holcomb (Br. 19, quoting p. 2 of the Final Rejection); (b) Holcomb does not generate a validation key using the second key (*id.*); and (c) Holcomb cannot teach the "first key" and "second key" claimed, because Holcomb states that "the microcontroller use[s] the same algorithm to calculate the codes" (Br. 20, quoting Holcomb, col. 1, ll. 37-38).

     In response, the Examiner argues that Holcomb discloses a first key, which drives the algorithm to produce the access code that is transferred from the key-generating station at the front desk to the programmable tag (Examiner's Ans. 14). According to the Examiner, the second key, which is the input that drives the algorithm to produce the code to the validation unit, is the second location that receives the generated key (Examiner's Ans. 14-15). The input to program the key is the first key, whereas the input to program the lock is the second key (*id.*).

We agree with Appellants. Claims 1 and 20 call for generating a first and second key for each access to the designated area. Holcomb teaches a key generating station at the front desk of a hotel, which encodes an access key code onto a magnetic media bearing card (FF 6). The electronic lock is equipped with a microcontroller, which (a) is hard-wired to the key generating station to receive the access key code from the station; (b) is equipped with the same algorithm as the key generating station, such that it can calculate the correct code; or (c) stores the same codes as the key generating station (FF 7). Each of these three alternatives means that the key code encoded onto the hotel guest's card, and the key code that the door's microcontroller seeks to match to the guest's card, are the same key (*i.e.*, the same code). Appellants' Specification makes clear that his first key and second key are not identical. Further, Appellants do not claim that the first key and second key are the keys to be compared when access is requested. However, because Appellants do not explicitly exclude the possibility that the *claimed* first and second keys are not identical, we must continue our analysis.

Claims 1 and 20 each recite "generat[ing] an access key using the first key" and "generat[ing] a validation key using the second key." Appellants disclose that the agent enters the agent key (as claimed, the "first key"), its agent code, the access date, and the customer's address into a programming unit, which in response generates an encrypted access key stored on the agent's programmable tag (FF 3). Similarly, the customer enters the customer key (the claimed "second key"), agent code, address of the designated area, and access date into the validation system, which then generates and stores an encrypted validation key, to be matched against the access key when it is presented (FF 4).

As noted *supra*, the Examiner's reading of Holcomb is that the first key "is the input that drives the algorithm to produce the access code that is transferred from the key-generating station at the front desk . . . to the programmable tag" (Examiner's Ans. 14), and the second key "is the input that drives the algorithm to produce the code to the validation unit (the electronic lock)" (Examiner's Ans. 15). This interpretation is erroneous because Appellants' claims call for generating a first and second key for each access to the designated area, generating an access key from the first key, *and* also generating a validation key from the second key. Holcomb does not contain sufficient "generating" activity to meet all these steps. The only "generating" in Holcomb occurs at the key generating station at the front desk, in which an access code for a room is generated and encoded onto a hotel guest's magnetic key card. There is no disclosure in Holcomb of the generation of an access key from the first key, because in Holcomb the first key *is* the access key, and no further activity is deemed necessary. There is no disclosure in Holcomb of the generation of a validation key from the second key, because in Holcomb the second key *is* the validation key, and no further activity is deemed necessary.

The Examiner's construction of the first and second keys as corresponding to the inputs to the code-generating algorithms of Holcomb fails to meet the claims, because there is no teaching of those algorithm inputs being *generated*. In Holcomb, ultimately, an access code is generated at the key generating station by a human operator, most likely by the press of a key on a computer keyboard. We decline to interpret that keypress as meeting "generating a first and second key for each access," according to the customary meaning of the activity disclosed and claimed by Appellants. Holcomb generates a (unitary) key for each access, which is encoded on a magnetic media-bearing card and also transmitted to an electronic lock mechanism. Because Holcomb fails to teach generating an access key using the first key or generating a validation key using the second key, we will reverse the Examiner's rejection of independent claims 1 and 20, as well as claims 2, 3 and 12 dependent therefrom.

With regard to the rejections under 35 U.S.C. § 103, we have reviewed the Lee, Porter, and Scott references. None of these references supplies the teachings absent from Holcomb, or anticipates any claim by itself. Therefore, we will reverse the Examiner's rejection of claims 4-11, 13-19 and 26-28.

CONCLUSION OF LAW

We conclude that Appellants have shown that the Examiner erred in rejecting claims 1-20 and 26-28. On the record before us, claims 1-20 and 26-28 have not been shown to be unpatentable.

DECISION

The Examiner's rejection of claims 1-20 and 26-28 is reversed.

REVERSED

tdl/gw

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER LLP
901 NEW YORK, AVENUE, NW
WASHINGTON, DC 20001-4413